JUSTER*: Jurnal Sains dan Terapan*
Vol. 4, No. 1, Januari 2025
p-ISSN: 2809-7661, e-ISSN: 2809-7750

Analisa Keamanan Data Pada Sistem Informasi Kampus (SISKA) Universitas Bina Darma Menggunakan Metode *Burp Suite*

Vicky Dwi Cahya[1*], Tamsir Ariyadi[2], Djeysen Kurniawan[3], Yovi Fajar Irfansyah[4]
[1,2,3,4]Universitas Bina Darma
Email Corespondent[*]: vickydwicahya11@email.com

Abstract

The Campus Information System (SISKA) is one of the important applications in managing academic data at Bina Darma University. Data security is a critical issue, especially in protecting sensitive information such as student data, class schedules, and academic results. This study aims to analyze data security on SISKA using Burp Suite, a web application security testing tool. The analysis process involves testing for authentication, authorization, and common vulnerabilities such as SQL Injection, XSS (Cross-Site Scripting), and data leakage. The test results show that there are several security holes that need to be fixed, including in user session management and input validation. Recommendations for improvement are provided to improve system security. The Campus Information System (SISKA) is one of the important applications in managing academic data at Bina Darma University. Data security is a critical issue, especially in protecting sensitive information such as student data, class schedules, and academic results. This study aims to analyze data security on SISKA using Burp Suite, a web application security testing tool. The analysis process involves testing for authentication, authorization, and common vulnerabilities such as SQL Injection, XSS (Cross-Site Scripting), and data leakage. The test results show that there are several security holes that need to be fixed, including in user session management and input validation. Recommendations for improvement are provided to improve system security.
Keywords*: Burp Suite, Data security, Penetration testing, SISKA, Vulnerability analysis*

Abstrak

Sistem Informasi Kampus (SISKA) adalah salah satu aplikasi penting dalam pengelolaan data akademik di Universitas Bina Darma. Keamanan data menjadi isu kritis, terutama dalam melindungi informasi sensitif seperti data mahasiswa, jadwal perkuliahan, dan hasil akademik. Penelitian ini bertujuan untuk menganalisis keamanan data pada SISKA menggunakan Burp Suite, sebuah alat pengujian keamanan aplikasi web. Proses analisis melibatkan pengujian terhadap autentikasi, otorisasi, dan kerentanan umum seperti SQL Injection, XSS (Cross-Site Scripting), dan kebocoran data. Hasil pengujian menunjukkan bahwa terdapat beberapa celah keamanan yang memerlukan perbaikan, termasuk pada pengelolaan sesi pengguna dan validasi input. Rekomendasi perbaikan disampaikan untuk meningkatkan keamanan sistem. Sistem Informasi Kampus (SISKA) adalah salah satu aplikasi penting dalam pengelolaan data akademik di Universitas Bina Darma. Keamanan data menjadi isu kritis, terutama dalam melindungi informasi sensitif seperti data mahasiswa, jadwal perkuliahan, dan hasil akademik. Penelitian ini bertujuan untuk menganalisis keamanan data pada SISKA menggunakan Burp Suite, sebuah alat pengujian keamanan aplikasi web. Proses analisis melibatkan pengujian terhadap autentikasi, otorisasi, dan kerentanan umum seperti SQL Injection, XSS (Cross-Site Scripting), dan kebocoran data. Hasil pengujian menunjukkan bahwa terdapat beberapa celah keamanan yang memerlukan perbaikan, termasuk pada pengelolaan sesi pengguna dan validasi input. Rekomendasi perbaikan disampaikan untuk meningkatkan keamanan sistem.
Kata Kunci: *Analisis kerentanan, Burp Suite, Keamanan data, SISKA, Uji penetrasi*

PENDAHULUAN

Di era digital yang terus berkembang ini, kebutuhan akan pengolahan data yang aman dan efektif akan menjadi prioritas utama, terutama bagi lembaga pendidikan seperti perguruan tinggi. Sistem Informasi Kampus (SISKA) Universitas Bina Darma merupakan salah satu infrastruktur teknologi yang digunakan untuk mendukung berbagai kegiatan akademik, administrasi, dan

operasional kampus. Perlindungan keamanan data merupakan aspek yang sangat penting, dengan beberapa fungsi krusial yang mendukung analisis data mahasiswa, dosen, keuangan, dan akademik.

SISKA telah diterapkan oleh Universitas Bina Darma untuk meningkatkan efisiensi operasional kampus. Meskipun demikian, ancaman seperti serangan siber, pelanggaran data, dan eksploitasi kerentanan dalam sistem informasi terus menimbulkan risiko nyata. Data yang buruk dapat menimbulkan konsekuensi serius, seperti penurunan reputasi institusi, gangguan penyedia layanan, dan klien pribadi. Oleh karena itu, perlu dilakukan evaluasi terhadap setiap aspek kinerja SISKA guna memastikan bahwa SISKA aman dari berbagai potensi ancaman.

Universitas Bina Darma telah mengalami ancaman keamanan nyata dalam sistem informasi kampusnya. Penelitian menunjukan bahwa website sistem informasi akademik sering mengalami downtime akibat tingginya akses yang membuka celah bagi peretasan. Upaya untuk meningkatkan sistem keamanan informasi terus dilakukan untuk mencegah serangan yang dapat merugikan kampus.

Statistik terkait keamanan data di universitas bina darma menunjukan rendahnya perhatian serius terhadap ancaman siber. Meskipun tidak ada angka spesifik yang di sebutkan dalam hasil pencarian, tantangan seperti downtime sistem informasi akibat serangan dan kerentanan yang teridentifikasi melalui pengujian penetrasi menunjukan perlunya peningkatan keamanan. Universitas juga menerapkan firewall dan intrusion detection system (IDS) untuk melindungi data akademik, yang mencerminkan komitmen mereka terhadap keamanan informasi di sektor pendidikan tinggi

Penelitian ini menggunakan metode Burp Suite, sebuah alat uji penetrasi yang dirancang untuk mendeteksi kelemahan keamanan dalam aplikasi berbasis web. Burp Suite memungkinkan analisis terhadap beberapa aspek keamanan, seperti validasi input, analisis sesi, dan pengodean data. Diharapkan kelemahan potensial di SISKA Universitas Bina Darma dapat diidentifikasi dan tindakan mitigasi yang tepat akan diterapkan melalui analisis keamanan menggunakan Burp Suite.

METODE

Penelitian ini dilakukan dengan pendekatan studi kasus yang berfokus pada Sistem Informasi Kampus (SISKA) Universitas Bina Darma. Meliputi Tahapan Penelitian:

1. Pengumpulan Data:

Struktur dan fungsi utama SISKA diidentifikasi menggunakan fitur Burp Suite untuk membuat arsitektur aplikasi web. Pengujian keamanan dan analisis kerentanan Sistem Informasi Kampus (SISKA) Universitas Bina Darma menggunakan Burp Suite menunjukkan hasil yang signifikan. Dalam pengujian ini, Burp Suite digunakan untuk memindai dan mengidentifikasi kerentanan, termasuk SQL Injection dan Cross-Site Scripting (XSS). Penelitian menemukan 17 jenis kerentanan, dengan beberapa di antaranya berada pada tingkat tinggi, seperti formulir HTML tanpa perlindungan CSRF. Rekomendasi perbaikan meliputi penerapan kontrol akses yang lebih ketat dan memperkuat enkripsi data untuk meningkatkan keamanan sistem.

2. Pengujian Keamanan:

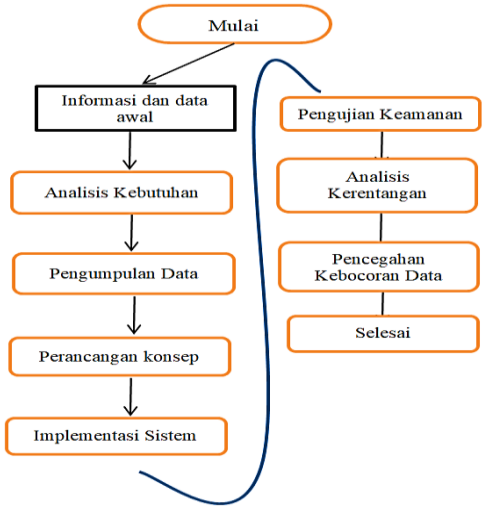
Lakukan penelitian tentang masalah keamanan utama seperti SQL Injection, *Cross-Site Scripting* (XSS), dan manajemen sesi menggunakan alat Burp Suite.

3. Analisis Kerentanan:

Menganalisis kerentanan yang dilakukan berdasarkan ambang batas dampakny dan keparahan sistem.

4. Rekomendasi Perbaikan

Menyediakan strategi mitigasi teknis untuk mengatasi masalah yang telah diidentifikasi.



Gambar 1. Alur penelitian

HASIL DAN PEMBAHASAN

Universitas Bina Darma menerapkan standar keamanan OWASP dan Siska untuk melindungi sistem informasi akademik. OWASP menyediakan kerangka kerja untuk mengidentifikasi dan mengatasi kerentanan melalui alat seperti OWASP ZAP, yang digunakan untuk pemindaian dan analisis keamanan. Penelitian menunjukkan bahwa 17 jenis kerentanan ditemukan, dengan rekomendasi untuk meningkatkan keamanan sistem.

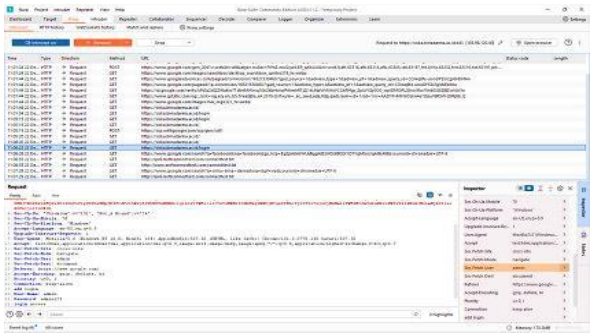
Siska, di sisi lain, lebih fokus pada konteks lokal dan spesifik terhadap kebutuhan institusi pendidikan, meskipun detail penerapannya tidak sebanyak OWASP. Kombinasi kedua pendekatan ini membantu meningkatkan kesadaran dan tindakan pencegahan terhadap ancaman siber di universitas.

1. Pengumpulan data pada Siska Bina Darma

Gambar 1. Burp *suite web*

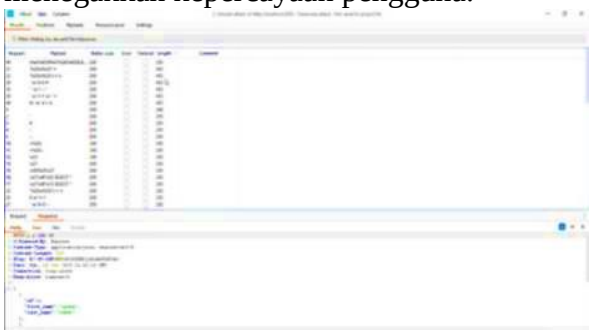
Mengidentifikasi web Sistem Informasi Kampus Bina Darma (siska) pada burp suite

2. Menguji keamanan



Gambar 2. Pengujian SQL

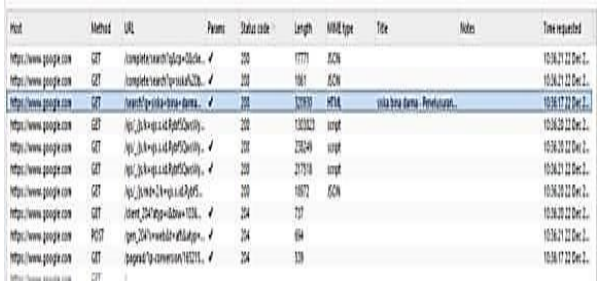
Melakukan pengujian akun dan password pada sistem informasi kampus dan dapat melihat kebocoran data. Setiap institusi yang menangani data sensitif harus mengutamakan pemeliharaan sistem informasi untuk mengurangi risiko dan menegakkan kepercayaan pengguna.



Gambar 3. Analisa SQL

Menganalisa kerentangan sql dapat menyerang melindungi yang di tuju dan dapat melihat data yang di tuju

3. Pencegahan kebocoran data



Gambar 4. Pencegahan data SQL

Pastikan semua komunikasi HTTP ke HTTPS ini akan memasitikan pencegahan penyadapan data selama web site berjalan. Kerentanan fungsi siska dapat memiliki

dampak spesifik yang signifikan, antara lain kehilangan data dikarenakan sistem yang tidak aman sehingga mengakibatkan hilangnya data penting akibat serangan siber atau kegagalan sistem, kerentanan dapat menyebabkan akses tidak sah ke data pribadi yang berpotensi mengakibatkan pelanggaran privasi.

KESIMPULAN

Penelitian ini berhasil menggunakan metode Burp Suite untuk mengidentifikasi beberapa kesalahan pada Sistem Informasi Kampus (SISKA) Universitas Bina Darma. Beberapa masalah utama yang disebutkan adalah SQL Injection, Cross-Site Scripting (XSS), Session Management Session, dan penanganan data sensitif. Ketegangan ini dapat menimbulkan risiko terhadap keamanan data dan fungsionalitas sistem.

Diharapkan penerapan langkah-langkah yang disarankan, seperti validasi input, peningkatan enkripsi, analisis sesi yang lebih menyeluruh, dan audit keamanan berkala, akan meningkatkan level SISKA. Dengan bantuan pedoman ini, Universitas Bina Darma dapat melindungi data sensitif mereka dan memastikan prosedur operasional yang aman dan transparan.

DAFTAR PUSTAKA

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno. com*, *22*(2).

Abdan, M. K. (2022). Pengujian Keamanan Sistem Informasi Berbasis Web Berdasarkan Framework Owasp Wstg V4. 2 (Studi Kasus: Sistem Sekawan V1 Universitas Islam Indonesia).

Basyirah, A., Hediyanto, U. Y. K. S., & Fathinuddin, M. (2023). Optimisasi Strategi Security Mitigation Dengan Vapt Pada Website Absensi Praktikan Dan Asisten Laboratorium Praktek. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *7*(2), 765-777.

Faizi, Z., & Ridha, A. A. (2023). Analisis Web Security Hole Menggunakan Metode Penetration Testing Execution And Standard (Studi Kasus: Universitas Singaperbangsa Karawang). *Jurnal Informasi dan Komputer*, *11*(02), 322-327.

Fajarino, A., Kunang, Y. N., Yudha, H. M., Negara, E. S., & Damayanti, N. R. (2023). Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *7*(2), 991-1005.

Ifani, A. Z., Aspar, N. F., Setiawan, A. D., & Azlam, M. (2024). Pengujian Keamanan Sistem Informasi Data Kependudukan Menggunakan Metode Pentetration Testing. *Jurnal Fokus Elektroda: Energi Listrik, Telekomunikasi, Komputer, Elektronika dan Kendali)*, *9*(2), 73-78.

Kuncoro, A. W., Fayruz Rahma, S. T., & ENG, M. (2022). Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review. *AUTOMATA*, *3*(1).

Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan sistem keamanan autentikasi single sign on (sso) menggunakan algoritma aes dan one-time password studi kasus: sso universitas ubudiyah indonesia. *Jurnal Rekayasa Elektrika*, *12*(1), 21-29.

Pormes, R., Wulan, P. I. D. C., Perdana, D. P., Fauzi, R., & Syahputra, A. Y. (2024). Analisis Keamanan Website E-Learning Politeknik Bhakti Semesta Berbasis Vulnerability Assessment. *Jurnal Jarkom*, *12*(02), 43-56.

Rafeli, A. I., Seta, H. B. & Widi, I. W. Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ. *Inform. J. Ilmu Komput.* **18**, 97 (2022).

Rainita, N. P. A., Athalia, A. A. I. C., Ananta, M. D. P., Pramana, I. K. P. T., Saskara, G. A. J., & Listartha, I. M. E. (2023). Analisis Perbandingan Vulnerability Scanning Pada Website Dvwa Menggunakan Owasp Nikto Dan Burpsuite. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *3*(2), 89-97.

Rosallah, Y. T. A. (2021). Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing Dan Metode OWASP (Open Web Application Security Project) Top 10 Pada Website Sistem Informasi Manajemen (SIM) Universitas Pembangunan Nasional Veteran Jakarta.

Subari, A., Manan, S., Ariyanto, E., & Fauzi, A. (2022). Pemanfaatan Metode Wavs (Web Application Security Scanners) Menggunakan Burp Suite Tools Dalam Audit Teknis Keamanan Sistem Informasi Surat Tugas Sekolah Vokasi Undip. *Gema Teknologi*, *21*(4).

Supriadi, D., Suryadi, E., Muslim, R., & Samsumar, L. D. (2024). Implementasi Vulnerability Assessment Owasp (Open Web Application Security Project) Pada Website Universitas Teknologi Mataram. *Journal of Data Analytics, Information, and Computer Science*, *1*(4), 232-240.

Tinambunan, F., Junaidi, A., & Rizki, A. M. (2024). Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 1062-1069.